IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF: **(1) Apple iPhone 16 ProMax, in a blue phone case** **(2) Samsung Galaxy, in a black Otterbox phone case** **(3) Samsung Phone, in a green Designskin phone case** CURRENTLY IN THE POSSESSION OF THE FBI AND LOCATED AT 2100 JAMIESON AVENUE, ALEXANDRIA, VA 22314	1:25-SW-342

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT

I, Samantha Wendt, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since June of 2023. I am currently assigned to the Washington Field Office. My primary duties include investigating violations of federal law, including securities fraud, wire fraud, bank fraud, and internet-enabled crimes. Part of those duties include investigating instances of wire fraud and bank fraud being used for financial gain at the expense of others.

2. Before my career as an FBI Special Agent, I was employed as a Forensic Accountant by the FBI in the Seattle Field Office for two years. I am a Certified Public Accountant and a Certified Fraud Examiner. As part of that role, I conducted the financial portion of investigations, which included reviewing financial records and determining the sources and uses

of funds. In that role, I was also part of the FBI's Virtual Currency Response Team as a specialist in blockchain analysis.

3. I have participated in numerous investigations related to financial crimes and have experience analyzing financial documents, interviewing suspects and witnesses, and reviewing evidence obtained from physical and digital search warrants. I have also participated in investigations that involve blockchain analysis and the seizure of cryptocurrencies.

4. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—various electronic devices further described in Attachment A—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

5. I have personally participated in this investigation and have witnessed many of the facts and circumstances described herein. The information set forth in this affidavit is based on my own personal knowledge, my review of relevant records, reliable information provided to me by other law enforcement personnel, interviews of victims and witnesses, and my training and experience. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Unless otherwise indicated, all written and oral statements referred to herein are set forth in substance and in part, rather than verbatim.

6. Based on my training, experience, and the facts as set forth in this affidavit, there is probable cause to believe that **JIHOON PARK** and others both known and yet unknown have committed violations of 18 U.S.C. § 157 (Bankruptcy Fraud), 18 U.S.C. § 1343 (Wire Fraud) and 18 U.S.C. § 1956(a)(1)(B)(i) (Concealment Money Laundering) (the "**SUBJECT OFFENSES**").

Further, based on my training, experience, and the facts as set forth in this affidavit, there is also probable cause to believe that examining the **TARGET DEVICES** associated with **PARK** will uncover evidence, fruits, and/or instrumentalities of the aforementioned criminal violations as more particularly described in Attachment B.

THE TARGET DEVICES

7. The property to be searched, collectively referred to as the **TARGET DEVICES**, which consist of the following devices confiscated from the **PARK** on April 17, 2025:

a. An Apple iPhone 16 ProMax in a blue phone case;

b. A Samsung Galaxy, in a black Otterbox phone case, with IMEI 352512143400313; and

c. A Samsung Phone, in a green Designskin phone case, IMEI 359186103322693.

8. On April 17, 2025, Fairfax County Police Department seized the **TARGET DEVICES** when they effectuated the arrest of **PARK** in Fairfax, Virginia. On April 17, 2025, **PARK** and the **TARGET DEVICES** were transferred to the custody of Fairfax County Sheriff's Office. **PARK** remained detained at the Fairfax County Sheriff's Office overnight. The **TARGET DEVICES** were stored overnight, along with **PARK**'s other personal property, at 10520 Judicial Dr, Fairfax, Virginia.

9. On April 18, 2025, **PARK** was released into the custody of the FBI from the Fairfax County Sheriff's Office. **PARK**'s personal property, including the **TARGET DEVICES**, were also transferred to the custody of the FBI. On multiple instances on April 18, 2025, **PARK** confirmed that he recognized and owned the **TARGET DEVICES**.

10. The **TARGET DEVICES** are currently in FBI custody, and stored at 2100 Jamieson Avenue, Alexandria, VA 22314.

JURISDICTION

11. This Court has jurisdiction to issue the requested warrants because the devices are located within the Eastern District of Virginia. Fed. R. Crim. P. 41.

BACKGROUND ON VIRTUAL CURRENCY

12. **Virtual Currency**: Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency, such as the U.S. dollar. Virtual currencies are not issued by any government- or bank-like traditional fiat currencies, but rather are generated and controlled through computer software. Bitcoin (BTC) and ether (ETH) are currently the most well-known virtual currencies in use. Tether (USDT) and USD Coin (USDC) are two stablecoins, meaning that their value is pegged to the United States dollar. In other words, one USDT equates to $1 and one USDC also equates to $1.

13. **Virtual Currency Address**: Virtual currency addresses are the particular virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of letters and numbers.

14. **Private Key**: Each virtual currency address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password, which is needed to access the address. Only the holder of a virtual currency address's private key can authorize a transfer of virtual currency from that address to another address.

15. **Virtual Currency Wallet**: There are various types of virtual currency wallets, including software wallets, hardware wallets, and paper wallets. A virtual currency wallet allows users to store, send, and receive virtual currencies. A virtual currency wallet can hold many virtual currency addresses at the same time. Wallets that are hosted by third parties are referred to as "hosted wallets" because the third party retains a customer's funds until the customer is ready to

transact with those funds. Conversely, wallets that allow users to exercise total, independent control over their funds are often called "unhosted wallets."

16. **Blockchain**: Many virtual currencies publicly record all of their transactions on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by the decentralized network of computers, containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction for each virtual currency address. There are different blockchains for different types of virtual currencies.

17. **Blockchain Explorer**: These explorers are online tools that operate as a blockchain search engine allowing users the ability to search for and review transactional data for any addresses on a particular blockchain. A blockchain explorer is software that uses API[1] and blockchain nodes to draw data from a blockchain and uses a database to arrange and present the data to a user in a searchable format.

18. **Virtual Currency Exchanges (VCEs)**: VCEs are trading and/or storage platforms for virtual currencies, such as BTC and ETH. Many VCEs store their customers' virtual currency in virtual currency wallets. As previously stated, these wallets can hold multiple virtual currency addresses associated with a single user. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers (*i.e.*, Know Your Customer ("KYC") checks) and to have anti-money laundering programs in place (to the extent they operate and service customers in the United States).

[1] API stands for application programming interface, which is a set of definitions and protocols for building and integrating application software.

19. **Blockchain Analysis:** As previously stated, while the identity of a virtual currency address owner is generally anonymous, law enforcement can identify the owner of a particular virtual currency address by analyzing the blockchain (*e.g.*, the BTC blockchain). The analysis can also reveal additional addresses controlled by the same individual or entity. "For example, when an organization creates multiple [BTC] addresses, it will often combine its [BTC] addresses into a separate, central [BTC] address (*i.e.*, a 'cluster'). It is possible to identify a 'cluster' of [BTC] addresses held by one organization by analyzing the [BTC] blockchain's transaction history. Open-source tools and private software products can be used to analyze a transaction." *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020).

20. In addition to using publicly available blockchain explorers, law enforcement uses commercial services offered by several different blockchain-analysis companies to investigate virtual currency transactions. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups involved in transactions. Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable.

PROBABLE CAUSE

21. I have probable cause to believe that, beginning on a date unknown, but by October 2018, and continuing through at least August 2024, **JIHOON PARK** devised and intended to devise a scheme to defraud individuals, including Victim-1, Victim-2, and Victim-3, by obtaining investments through materially false and fraudulent pretenses, representations, and promises. **PARK** met with Victim-1, Victim-2, and Victim-3 in person, including in the Eastern District of Virginia, and communicated with Victim-1, Victim-2, and Victim-3 through electronic communications and by telephone. As part of the scheme, **PARK** misrepresented the manner in which the funds obtained from defrauded individuals, specifically Victim-1, Victim-2, and Victim-3, would be used.

22. According to records obtained from Massachusetts Mutual Life Insurance Company ("MassMutual"), **PARK** was employed with MassMutual from approximately October 2013 through no later than June 2023. The Financial Industry Regulatory Authority ("FINRA") terminated **PARK**'s registration as a registered representative of MassMutual as of December 31, 2022. As part of the termination, **PARK** was required to promptly remove references and affiliations with MassMutual from social media platforms, websites and communications. However, even after **PARK** was no longer employed at MassMutual, he misled victims about his employment status with MassMutual to further gain their trust and provide legitimacy to his financial advice.

I) Victim-1

23. Victim-1 is a resident of the Eastern District of Virginia and is currently 60 years old. Victim-1 was acquainted with **PARK** for approximately 20 years. **PARK** attended the same church as Victim-1. Victim-1 said she trusted **PARK**.

24. Victim-1 was awarded approximately $1.6 million in a divorce settlement. In 2021, **PARK** was presented to Victim-1 as someone who could provide financial advice when Victim-1 received the divorce settlement in approximately April 2022.

25. In approximately August 2021, Victim-1 met with **PARK** to discuss investments. Victim-1 did not want to invest in stocks due to price fluctuations. **PARK** explained that cryptocurrency was a good investment option. **PARK** explained that there was little risk to Victim-1's investments, claiming that the principal amount would never go away. **PARK** told Victim-1 that she would earn 7% compound interest per month. Victim-1 was also told that she would be able to withdraw the interest at any time.

26. From September 2021 through December 2021, **PARK** claimed to help Victim-1 make several transfers for her investment. The transfers occurred by moving money from Victim-1's bank accounts to a Coinbase account in Victim-1's name. **PARK** and Victim-1 would go to the bank together to initiate the wire transfers from Victim-1's bank account to Coinbase. Victim-1 invested approximately $400,000 at this time. Victim-1 believed that her money was invested with MassMutual and **PARK** told her that MassMutual used Coinbase.

27. **PARK** instructed Victim-1 to purchase a tablet so that Victim-1 could access an application for her investments. Victim-1 later learned that the application for her investments was called KOK Play.[2] **PARK** told Victim-1 to not search KOK Play on Google and to not open her cryptocurrency applications because it would make the applications susceptible to hackers. Victim-1 rarely checked her accounts. Victim-1 recalled asking **PARK** if KOK Play was a pyramid scheme, and **PARK** stated that it was not. Victim-1 recalled that **PARK** stated KOK Play was associated with MassMutual.

28. In April 2022, Victim-1 received the divorce settlement. Victim-1 wanted to purchase a residence with the divorce settlement money. **PARK** advised that it was not a good time to purchase a residence, and that Victim-1 should instead invest in other entities. Based on this advice, Victim-1 moved $1,090,000 to Coinbase. An additional $200,000 transfer from

[2] Keystone of Opportunity & Knowledge (KOK) purported to be a digital content distribution platform that would create and develop its own media, videos, games, and blockchain. KOK Play was the mobile application associated with KOK. According to KOK promotional materials, KOK's business model was to primarily generate revenue from the content on its platform and advertisements. KOK created their own virtual currency, "KOK Coins," to be used as currency on their platform. KOK's actual revenue appeared to come from recruiting new investors.

Victim-1 to Coinbase failed, so **PARK** requested the $200,000 in a cashier's check instead, which he subsequently deposited on May 4, 2022.

29. Victim-1 reported asking **PARK** in June 2023 if he was still employed with MassMutual and **PARK** responded yes. Victim-1 then called MassMutual, who stated that **PARK** no longer worked there.

30. Victim-1 invested with **PARK** because she thought she could withdraw funds whenever she wanted. When Victim-1 tried to withdraw funds, **PARK** told her that she needed to wait two or three years. Victim-1 has repeatedly asked **PARK** for her money back. To date, **PARK** has provided Victim-1 less than $100,000. Victim-1 was unable to access her own funds because she did not know how to withdraw the funds herself from KOK Play.

31. Victim-1 reported meeting with **PARK** in person and communicating with **PARK** via telephone. To communicate, **PARK** and Victim-1 used the mobile application KakaoTalk[3] and email at luciuspark@gmail.com ("**PARK**'s Google email address").

32. I have obtained and reviewed financial records and VCE account records for Victim-1 and **PARK**. Between September 2021 and May 2022, Victim-1 transferred approximately $1,660,000, including $1,460,000 to Coinbase and $200,000 to Wells Fargo account number ending in -6021, in the name of **JI H PARK** ("**PARK**'s Wells Fargo Account"). Information provided from Wells Fargo confirms the account is owned by **PARK**. Of the money transferred to Coinbase:

[3] KakaoTalk is a mobile messaging application operated by Kakao Corporation, a South Korean internet company. The most effective way to get the content of KakaoTalk messages is by obtaining the device, in this case a mobile telephone, that is using the application.

a. In September 2021, approximately 94 ETH, worth approximately $300,000, was moved via the blockchain to cryptocurrency addresses that appeared to be associated with KOK Play.

b. In April 2022, approximately 980,000 USDT, worth approximately $980,000, was transferred to a KuCoin[4] account. Records obtained from KuCoin indicated that the account was associated with **PARK**'s Google email address and a telephone number associated with **PARK**.

33. A review of **PARK**'s Wells Fargo Account indicated that the $200,000 cashier's check from Victim-1 was deposited on or around May 4, 2022. There were no additional deposits or withdrawals from **PARK**'s Wells Fargo Account until January 23, 2023, when a cashier's check was made payable to Victim-1. In total, Victim-1 received three cashier's checks from **PARK** totaling $94,000 as a return of her investment funds. The only other withdrawal from **PARK**'s Wells Fargo Account in 2022 and 2023 was a $4,770 purchase at a luxury retail store located in McLean, Virginia. Based on my review of the financial statements, it did not appear that Victim-1's $200,000 cashier's check was invested.

II) Victim-2

34. Victim-2 is a resident of the Eastern District of Virginia and is currently 72 years old. Victim-2 reported speaking with **PARK** in person, including in the Eastern District of Virginia, and via KakaoTalk.

[4] KuCoin is a VCE located in the Seychelles.

35. In 2023, Victim-2 was introduced to **PARK** associated with FileUp, a global cryptocurrency mining service provider.[5] **PARK** described FileUp as a pyramid organization and a multi-level marketing company. **PARK** purported to be the top of FileUp within the United States. Victim-2 did not want to invest in FileUp through **PARK**, but **PARK**'s high status with FileUp was one of the reasons why Victim-2 trusted **PARK**.

36. **PARK** also introduced himself to Victim-2 as an employee of MassMutual and an investment specialist. Similar to Victim-1, Victim-2 reported that **PARK**'s profile picture associated with his KakaoTalk account was an image of **PARK**'s MassMutual business card, indicating that **PARK** is a Managing Partner. **PARK** further indicated that one of the locations Victim-2 and **PARK** met at was the first floor of MassMutual. Victim-2 stated that he trusted **PARK** because of the information that **PARK** would have about financial markets due to **PARK**'s job with MassMutual.

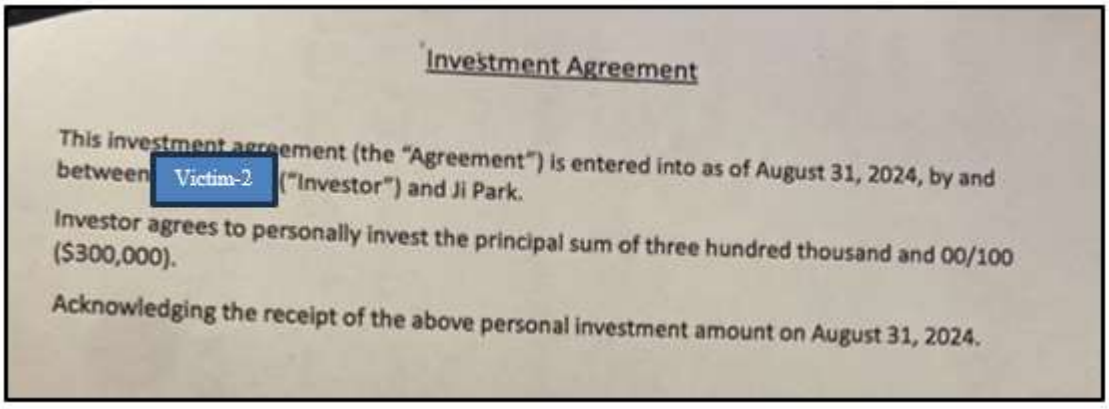
37. In March 2023, a $95,000 check from Victim-2 was deposited into **PARK**'s Wells Fargo Account. Victim-2 understood this check to be an investment related to cryptocurrency. Victim-2 provided the check to his neighbor. A review of **PARK**'s Wells Fargo Account indicated that the $95,000 check from Victim-2 was deposited on or around March 20, 2023. After the deposit from Victim-2, the only other withdrawals from **PARK**'s Wells Fargo Account in 2023 totaled less than $80,000 and comprised of funds being returned to Victim-1 and a purchase at a luxury retail store located in McLean, Virginia. The next withdrawal from **PARK**'s Wells Fargo Account was in or around September 2024 and comprised of a $700,000 purchase at Potomac Title Group associated with the purchase of **PARK**'s residence in Chantilly, Virginia ("**PARK's**

[5] According to https://www.fileup.global, FileUp is associated with the mining of Filecoin and Aleo, both cryptocurrency tokens.

RESIDENCE"). Based on my review of the financial statements, it did not appear that Victim-2's $95,000 check was invested in cryptocurrency.

38. In or around August 2024, **PARK** told Victim-2 that **PARK** had an investment opportunity for Victim-2, and Victim-2 needed to act quickly to take advantage of it. **PARK** indicated that an investment portfolio associated with the investment would be provided at a later date. **PARK** indicated that there would be a high rate of return. At the end of August 2024, Victim-2 invested $300,000 with **PARK**. At the time, Victim-2 still believed **PARK** worked at MassMutual but this was over one year after **PARK**'s employment with MassMutual ended. Victim-2 stated that he would not have invested with **PARK** if **PARK** did not work for MassMutual.

39. After investing, Victim-2 began to ask **PARK** for documentation associated with the investment. **PARK** indicated that the investment portfolio would include investments in: (i) ETF's / the S&P 500, (ii) real estate, and (iii) cryptocurrency. **PARK** provided, in part, the following documentation to Victim-2 to memorialize the investment:



Investment Agreement

This investment agreement (the "Agreement") is entered into as of August 31, 2024, by and between Victim-2 ("Investor") and Ji Park.

Investor agrees to personally invest the principal sum of three hundred thousand and 00/100 ($300,000).

Acknowledging the receipt of the above personal investment amount on August 31, 2024.

40. **PARK** told Victim-2 that Victim-2 could withdraw funds at any time. As recently as January 2025, Victim-2 tried to use **PARK**'s offer to withdraw their funds. **PARK** has not provided any funds to Victim-2.

41. On or around August 31, 2024, **PARK** deposited Victim-2's $300,000 check into Bank of America account number ending in -5371, in the name of JONG YON KIM ("KIM"), **PARK**'s spouse, and **JI HOON PARK** ("**PARK**'s Bank of America Account"). The balance in **PARK**'s Bank of America Account was less than $70,000 prior to the deposit from Victim-2. On or around September 12, 2024, $300,000 was transferred, via check, from **PARK**'s Bank of America Account to **PARK**'s Wells Fargo Account. Around that time, **PARK**'s Bank of America Account received less than $3,000 in deposits between the deposit of Victim-2's investment check and the transfer of $300,000 to **PARK**'s Wells Fargo Account. On September 23, 2024, **PARK**'s Wells Fargo Account wired $700,000 to Potomac Title Group. There were no additional deposits into **PARK**'s Wells Fargo Account prior to the transfer to Potomac Title Group and the balance in **PARK**'s Wells Fargo Account was less than $5,000 after the transfer.

42. I obtained records from Potomac Title Group associated with **PARK's RESIDENCE**. The records indicated that on September 30, 2024, **PARK** and KIM purchased **PARK's RESIDENCE** for $1,235,000. The property purchased was financed with $700,000 from **PARK**'s Wells Fargo Account and a $535,000 mortgage. **PARK** is listed on the Deed of Trust associated with **PARK's RESIDENCE**. Victim-2 indicated that they would not have been okay with **PARK** using their investment to purchase a house.

III) Victim-3

43. Victim-3 is a resident of Potomac, Maryland and is currently 51 years old.

44. Victim-3 reported investing approximately $900,000 with **PARK** in late 2018 and early 2019. **PARK** explained this investment as being in stocks that had not yet gone public. **PARK** told Victim-3 that it would be a three-year investment, the principle was guaranteed, and that Victim-3 would earn 20% interest. Victim-3 did not believe these investments were in

cryptocurrency and would not have invested in cryptocurrency at that time. Approximately one year before this investment was supposed to mature, **PARK** told Victim-3 that COVID-19 delayed the investments, and they would not be repaid until 2025. A review of **PARK**'s Wells Fargo Account indicated that a $300,000 wire transfer from Victim-3 was deposited on January 17, 2019. On the same day, a $270,000 outgoing wire to **PARK**'s account at Coinbase was conducted. The balance in **PARK**'s Wells Fargo Account prior to the deposit from Victim-3 was less than $30,000, indicating that the transfer to Coinbase was comprised of Victim-3's funds. A review of **PARK**'s Coinbase account indicated that between October 2018 and December 2018, **PARK**'s Coinbase account received $582,480 in additional deposits from **PARK**'s Wells Fargo Account. Together, the approximately $850,000 moved from **PARK**'s Wells Fargo Account to **PARK**'s Coinbase account between October 2018 and January 2019 is consistent with the time period that Victim-3 indicated she invested $900,000 with **PARK**.

45. In March 2023, Victim-3 invested an additional $125,000 with **PARK**. This was a five-year investment in cryptocurrency. Prior to this investment, Victim-3 had the funds in an account at MassMutual, where **PARK** was her account manager. **PARK** told Victim-3 she should move the funds from MassMutual to this cryptocurrency investment suggested by **PARK**. Victim-3, with **PARK**'s assistance, cashed out her MassMutual account to her bank account, and then obtained cashier's checks payable to **PARK** for this investment.

46. When Victim-3 asked **PARK** for statements or information associated with how the investments were doing, **PARK** indicated he could not provide that information since it was a group investment. Victim-3 was not provided a contract for the investments.

47. **PARK** explained the cryptocurrency investment opportunity to Victim-3 in his MassMutual office. **PARK** did not provide many details of Victim-3's investments through

KakaoTalk, text message, or email. **PARK** primarily communicated information associated with Victim-3's investment verbally.

48. Financial analysis related to the $125,000 transfer from Victim-3 in March 2023 did not indicate that the funds were used to invest in cryptocurrency, as **PARK** had promised. Instead, the funds remained idle in **PARK**'s Wells Fargo Account until September 2024, when they were combined with funds from Victim-1 and Victim-2 and used to purchase **PARK's RESIDENCE**.

IV) Financial Analysis Associated with PARK

49. Financial analysis conducted to date associated with **PARK**'s bank accounts and VCE accounts indicates that investor funds did not appear to be used for the benefit of the investors. At times, the funds moved through a series of accounts associated with **PARK** and KIM. Financial analysis conducted to date indicates that investor funds primarily appeared to fund the purchase of **PARK's RESIDENCE** and cryptocurrency stored within unhosted addresses inaccessible to victims.

PARK's Wells Fargo Account

50. Prior to January 14, 2019, **PARK**'s Wells Fargo Account had a balance less than $30,000. From January 14, 2019 through November 26, 2024, **PARK**'s Wells Fargo Account received $1,098,400 in deposits, as outlined below:

a. $425,000 from Victim-3.

b. $300,000 from **PARK**'s Bank of America Account.

c. $200,000 from Victim-1.

d. $95,000 from Victim-2.

e. $66,400 in cash deposits. Review of the cash deposits indicated that they were structured to be under $10,000, avoiding the filing of Currency Transaction Reports. For example, $9,000 was deposited in cash each day on March 22, 2023, March 23, 2023, March 24, 2023, March 27, 2023, March 28, 2023, and March 29, 2023. Additionally, on June 11, 2024, an $8,900 cash deposit was conducted at 02:41:13 p.m. and less than one minute later at 02:41:59 p.m. another $3,500 cash deposit was conducted at the same location in Fairfax, VA.

f. $12,000 from S.J., an individual residing in Warrington, PA. The memo lines of the checks indicated they related to cryptocurrency coins, which appears to indicate that the checks were intended to be invested.

51. In total, between January 14, 2019 and September 2024, **PARK**'s Wells Fargo Account appeared to receive over $1,000,000 in investor funds. These funds primarily appeared to be used for **PARK**'s benefit. From January 14, 2019 through November 26, 2024, **PARK**'s Wells Fargo Account conducted approximately $1,127,000 in withdrawals, including the below:

a. $700,000 to Potomac Title Group associated the purchase of **PARK**'s **RESIDENCE**.

b. $270,000 to **PARK**'s Coinbase account.

c. $94,000 to Victim-1.

d. $45,000 to MassMutual.

e. $5,200 in cash withdrawals.

f. $4,770 to Prada.

52. The balance in **PARK**'s Wells Fargo Account on May 1, 2022, was less than $5,000. Deposits into **PARK**'s Wells Fargo Account after that date totaled $798,400. Of those

deposits, $720,000 derived directly or indirectly from Victim-1, Victim-2, and Victim-3. Accordingly, such funds necessarily comprised the bulk of **PARK**'s transfer to Potomac Title Group associated with the purchase of **PARK's RESIDENCE**.

PARK's Coinbase Account

53. On January 17, 2019, **PARK**'s Coinbase Account received $270,000 from **PARK**'s Wells Fargo Account. These funds derived from Victim-3's $300,000 deposit on January 17, 2019. The balance in **PARK**'s Wells Fargo Account prior to the deposit from Victim-3 was less than $30,000. No other deposits were received prior to the $270,000 withdrawal to **PARK**'s Coinbase account. From there, the funds were moved in a manner that appeared designed to conceal the source of the funds, as described below:

a. On January 27, 2019, $269,990 was converted to 269,990 USDC, a cryptocurrency stablecoin. On that same date, 269,990 USDC was sent to KIM's Binance.com Account.

b. On January 28, 2019, KIM's Binance.com Account converted approximately 269,835 USDC into approximately 77.43 BTC. On September 5, 2019, approximately 1 BTC was sent to **PARK**'s Bittrex[6] Account. On September 7, 2019, approximately 76.35 BTC was sent to **PARK**'s Bittrex Account.

c. On January 3, 2020, **PARK**'s Bittrex Account sent approximately 77.35 BTC to **PARK**'s Binance.US[7] Account.

---

[6] From approximately 2014 until 2023, Bittrex Global was a cryptocurrency exchange platform based in Seattle, Washington.

[7] Since approximately 2019, BAM Trading Services, Inc. operates as Binance.US, a cryptocurrency exchange platform based in Miami, Florida.

d. On June 13, 2020, **PARK**'s Binance.us Account sent two transactions, totaling approximately 77.35 BTC, back to **PARK**'s Coinbase Account. **PARK**'s Coinbase Account had a balance of approximately 36 BTC prior to these transactions.

e. On June 14, 2020, **PARK**'s Coinbase Account sent approximately two transactions, totaling approximately 40.1 BTC to KIM's Coinbase Account. KIM's Coinbase Account had a balance of approximately 10.5 BTC prior to these transactions.

f. Between December 25, 2021 and January 4, 2022, **PARK**'s Coinbase Account sent approximately 50 BTC to 10 unhosted addresses. On October 12, 2022, **PARK**'s Coinbase account sent approximately 23.34 BTC to another unhosted address. Blockchain analysis indicates these funds did not move from the addresses initially funded until April 8, 2025.

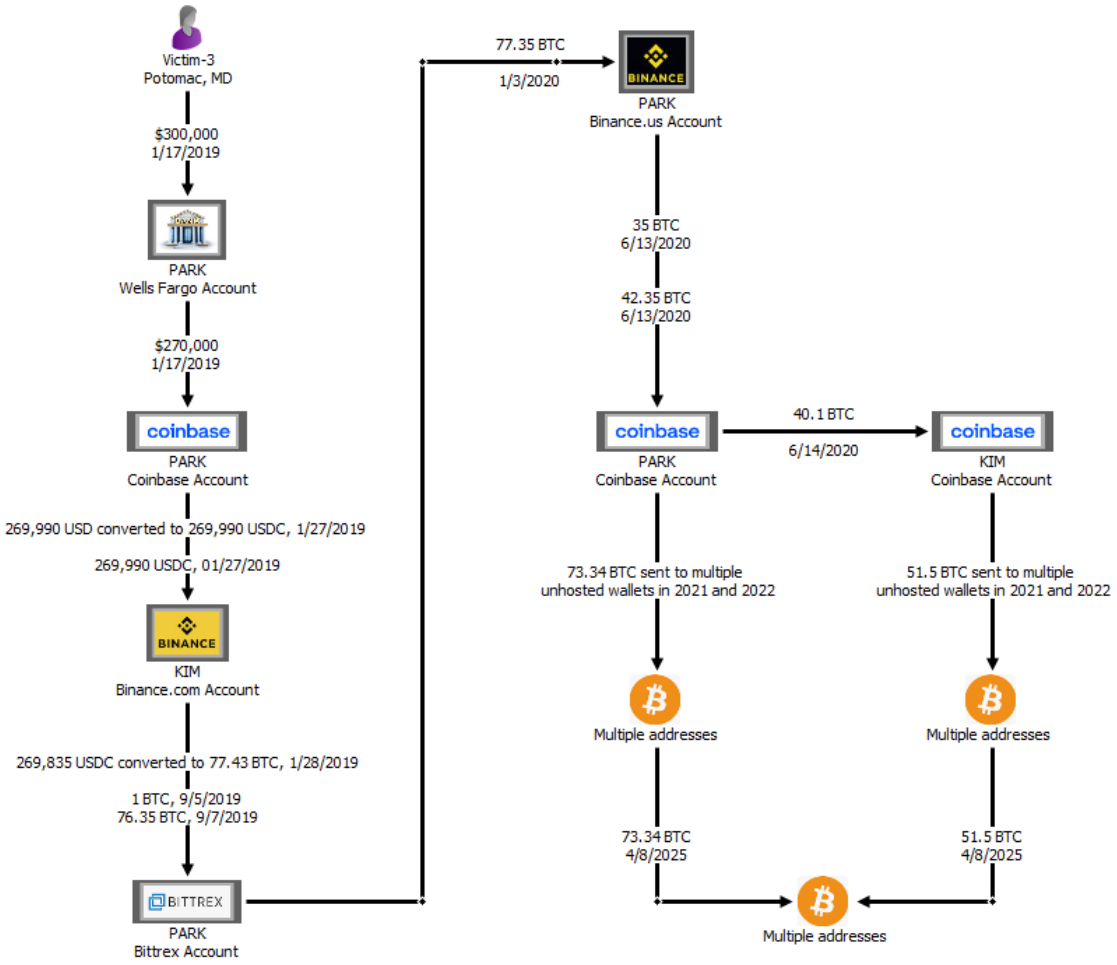
g. Between December 25, 2021 and January 5, 2022, KIM's Coinbase Account sent approximately 51.50 BTC to 11 unhosted addresses. Blockchain analysis indicates these funds did not move from the addresses initially funded until April 8, 2025.

h. On April 8, 2025, the unhosted addresses holding the bitcoin derived from **PARK**'s Coinbase Account and KIM's Coinbase Account consolidated into four new unhosted addresses.

54. Thus, approximately 77 BTC, estimated to be worth over $6 million,[8] held in unhosted addresses directly funded by **PARK**'s Coinbase Account and KIM's Coinbase Account

[8] As of April 2, 2025, CoinMarketCap indicated that 1 BTC equated to approximately $84,000.

appeared to derive from funds provided by Victim-3. The flow of funds described above is depicted below[9]:



PARK's KuCoin Account

55. On April 20, 2022, approximately 979,667 USDT was moved from Victim-1's Coinbase account to **PARK**'s KuCoin Account. I obtained records from KuCoin related to **PARK**'s KuCoin Account. Of note, **PARK**'s KuCoin Account records contained data starting on

[9] The amounts shown are approximations. The graphic does not represent all activity associated with the accounts and addresses.

April 26, 2022, several days after the receipt of funds from Victim-1. Based on my training and experience, I believe that review of the **TARGET DEVICES** may reveal **PARK**'s full KuCoin account history.

56. Based on review of the KuCoin records provided, **PARK**'s KuCoin Account only received one additional deposit in 2022—approximately 909 KOK Coins. In 2022, **PARK**'s KuCoin Account conducted the following transactions, in part:

a. Converted approximately 161,000 USDT to approximately 62,812 KOK Coins. Blockchain analysis indicates that these funds went to the same unhosted address and that the funds have not moved. These funds are estimated to now be worth less than $15.[10]

b. Converted approximately 75,000 USDT to approximately 52 ETH. Blockchain analysis indicates that approximately 51.1 ETH went to the same unhosted address and that the funds did not move until April 8, 2025. These funds are estimated to now be worth approximately $95,000.[11]

c. Converted approximately 75,000 USDT to approximately 202,000 Ripple (currency code: XRP), another type of virtual currency. Blockchain analysis indicates that approximately 195,000 XRP[12] went to the same unhosted address and

[10] As of April 2, 2025, CoinMarketCap indicated that 1 KOK equated to approximately $0.0002.

[11] As of April 2, 2025, CoinMarketCap indicated that 1 ETH equated to approximately $1,800.

[12] Some of the withdrawals occurred in 2023. However, **PARK**'s KuCoin Account records indicated no deposits were received in the form of XRP and that no additional conversions to XRP occurred.

that the funds did not move until April 8, 2025. These funds are estimated to now be worth approximately $400,000.[13]

57. Review of **PARK**'s KuCoin Account did not indicate activity consistent with investing Victim-1's funds.

58. Between January 2019 and September 2024, **PARK** received over $1 million directly from Victim-1, Victim-2, and Victim-3 into bank accounts controlled by **PARK**. In addition, **PARK** directed Victim-1 to move over $1.4 million to a Coinbase account in her name. Approximately $1 million of those funds were sent directly to **PARK**'s KuCoin account. **PARK**'s financial records indicate that instead of investing the funds on behalf of the investors, **PARK** purchased a house and appears to be storing the equivalent of millions of dollars in unhosted wallets. Victims have reported being unable to withdraw or recover their funds from **PARK** during this time period.

V) PARK's Chapter 7 Bankruptcy Filing

59. I have obtained and reviewed court records associated with a January 2025 Chapter 7 bankruptcy filed by **PARK**. Based on my training, knowledge, and experience, I believe that the bankruptcy filing represents an attempted by **PARK** to conceal assets, including **PARK's RESIDENCE**, and escape accountability to Victim-1 and Victim-2 associated with their investments.

60. On or around October 24, 2024, Victim-1 filed a civil case with Fairfax County Circuit Court related to her investment. On or around October 31, 2024, **PARK** was served with a copy of the complaint. On November 25, 2024, **PARK** received a Certificate of Counseling from

[13] As of April 2, 2025, CoinMarketCap indicated that 1 XRP equated to approximately $2.

Credit Advisors Foundation in preparation for filing for bankruptcy. On January 14, 2025, **PARK** filed for Chapter 7 bankruptcy with the United States Bankruptcy Court for the Eastern District of Virginia.

61. **PARK**'s Chapter 7 bankruptcy filings included Victim-1 and Victim-2 as creditors. The other creditors were financial institutions, such as American Express and JP Morgan Chase, and BMW of North America. **PARK** reported approximately $250,000 in funds owed to creditors. Of note, **PARK** did not include Victim-3 as a creditor.

62. **PARK**'s Chapter 7 bankruptcy filings initially indicated that: (i) **PARK** owned no real estate and, (ii) **PARK** lived at the **TARGET RESIDENCE** from 2016 through 2025. Both representations are inaccurate. As discussed above, **PARK's RESIDENCE** was purchased in September 2024. **PARK**'s name is listed on the Deed of Trust associated with the **PARK's RESIDENCE**.

63. On February 20, 2025, there was a 341(a) Meeting of the Creditors associated with **PARK**'s Chapter 7 bankruptcy filing. I have obtained and listened to a recording of the hearing. During the hearing, **PARK** indicated that his Chapter 7 bankruptcy filings contained inaccuracies. Notably, during the hearing, indicated that he did own real estate—**PARK's RESIDENCE**. **PARK** indicated that he acquired the residence in September 2024, not in 2016. **PARK** stated that he used Victim-2's funds towards the purchase of **PARK's RESIDENCE**. **PARK** characterized the investment from Victim-2 as borrowed funds that would be paid back in three-to-five years. **PARK** stated that he did not owe Victim-1 any money. **PARK** also claimed that he has not owned, bought, or traded cryptocurrency in the last two years.

64. On February 28, 2025, **PARK** filed an amendment to his Chapter 7 bankruptcy filings. **PARK** now indicated that he owned **PARK's RESIDENCE** and a 2016 Honda Odyssey.

PARK did not indicate ownership interest in a 2022 BMW. Records from the Virginia Department of Motor Vehicles ("DMV") indicated that a 2022 BMW was registered to **PARK**. In February 2025, the FBI has observed **PARK** driving the BMW.

65. On March 21, 2025, there was a second 341(a) Meeting of the Creditors associated with PARK's Chapter 7 bankruptcy filing. I have obtained and reviewed a transcript of this hearing. During the hearing, **PARK** stated that, in 2022, he did not receive any cryptocurrencies that were paid out of Victim-1's Coinbase account. As discussed above, this is false. During the hearing, **PARK** also stated that Victim-2's $300,000 investment related to **PARK**'s cosmetic business in South Korea. In an interview with law enforcement, Victim-2 stated he was not aware of **PARK**'s cosmetic business.

VI) The TARGET DEVICES

66. On September 11, 2024, I obtained records from Google associated with a 2703(d) Court Order for email address luciuspark@gmail.com.[14] Device details associated with **PARK**'s Google account indicated that it was associated with a Samsung Galaxy S7 Edge smartphone. As further described in Attachment A, one of the **TARGET DEVICES** appears to be a Samsung Galaxy. The records from Google indicated that several cryptocurrency related applications were downloaded onto the device, including Coinbase, KuCoin, KOK Play, Crypto.com, Bakkt, Trust, and BitGlobal.

67. **PARK**'s Google account further indicated that it was associated with several end-to-end encrypted messaging applications, including KakaoTalk, WeChat, and Telegram. Victim-

[14] I am familiar with **PARK** utilizing the name Lucius Park. Notably, Victim-1 referred to **PARK** as Lucius and reported communicating with **PARK** using this email address.

1 and Victim-2 reported communicating with **PARK** via KakaoTalk. Victim-2 provided a copy of KakaoTalk messages from **PARK** dated December 10, 2024.

68. On July 29, 2023, AT&T provided records associated with a phone number associated with **PARK**. The subscriber information indicated that the phone number had been registered to KIM as of June 2006. Victim-1 reported using the phone number to communicate with **PARK**. Toll records through July 6, 2023 indicated the following activity associated with **PARK**'s phone number:[15]

a. Between September 8, 2021 and June 15, 2023, Victim-1 and **PARK**'s phone number exchanged over 200 text messages and phone calls.

b. In April 2023, Victim-2 and **PARK**'s phone number exchanged two text messages and one phone call.

c. Between January 2020 and June 2023, Victim-3 and **PARK**'s phone number exchanged over 700 text messages and phone calls.

d. Between January 2020 and June 2023, S.J. and **PARK**'s phone number exchanged over 300 phone calls.

69. Based on my training, knowledge, and experience, I know that those who commit financial fraud and money laundering often use computers and mobile electronic devices (including cell phones and smartphones), device features (including photos, voice calls, text messages, and e-mails), and electronic accounts (such as e-mail and social media accounts) to store

[15] Based on the investigation conducted to date, I understand that **PARK** communicated with Victim-1 and Victim-2 through KakaoTalk, a mobile and web-based application. Text messages and phone calls exchanged through KakaoTalk are not included in the toll records provided by T-Mobile.

information and to communicate with others in furtherance of their crimes. As discussed above, Victim-1 and Victim-2 indicated that they communicated with **PARK** utilizing KakaoTalk. Such electronic devices and accounts allow participants in fraud schemes to transmit compromised identity and financial information, to direct and coordinate activities in furtherance of the conspiracy across substantial distances, and to conduct illicit financial transactions, including the types of financial and cryptocurrency transactions described above. I believe that examination of the **TARGET DEVICES** will identify communications with Victim-1, Victim-2, Victim-3, S.J., and other potential victims associated with **PARK**. I also believe that it will identify communications between **PARK** and potential co-conspirators associated with the scheme.

70. In my training and experience, data obtained from the electronic devices and accounts of those involved in financial fraud (such as e-mails, instant messages, contacts, location data, and photos) has enabled law enforcement to identify co-conspirators, victims, bank accounts, and cryptocurrency addresses used to store and transfer proceeds of the fraudulent activity. Internet search and browsing history associated with an electronic account can provide evidence of activities in furtherance of financial fraud and identity fraud, such as searching and browsing bank websites, to check bank account balances, to check blockchain explorers and to conduct transactions using fraud proceeds.

71. Electronic devices and accounts also commonly contain indicia of ownership and information identifying users of the devices and accounts. For example, I know that cryptocurrency addresses, private keys (akin to an account password), and seed phrases (akin to a master key) can be stored on mobile devices. The foregoing information is commonly maintained within the electronic device and account for substantial periods of time, to include several months and even years, and constitutes evidence and instrumentalities of the aforementioned crimes.

72. Based on my training and experience, I believe that an examination of the **TARGET DEVICES** is likely to reveal evidence regarding communications and records associated with **PARK** and additional co-conspirators and victims linked to the fraud scheme.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

73. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods. Similarly, things that have been viewed via the Internet are typically stored for some period on the device. This information can sometimes be recovered with forensics tools.

74. There is probable cause to believe that things that were once stored on the **TARGET DEVICES** may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer or other electronic device, such as a cellular telephone, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition,

a computer's or cellular telephone's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

75. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **TARGET DEVICES** were used, the purpose of their use, who used them, and when.

76. There is probable cause to believe that this forensic electronic evidence might be on the **TARGET DEVICES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review

team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

77. *Nature of examination.* Based on the foregoing and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **TARGET DEVICES** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

[This space intentionally left blank.]

CONCLUSION

78. Based on the foregoing, I respectfully submit that probable cause exists to believe **PARK** and others both known and yet unknown have committed the **TARGET OFFENSES** and that evidence, contraband, fruits, and instrumentalities of such crimes (as described in Attachment B) may be located on the **TARGET DEVICES** (as described in Attachments A).

Respectfully submitted,

Samantha Wendt

Samantha Wendt
Special Agent
Federal Bureau of Investigation

Subscribed to and sworn before me in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 18th day of April 2025.

William E. Fitzpatrick

Hon. William E. Fitzpatrick
United States Magistrate Judge

ATTACHMENT A

PROPERTY TO BE SEARCHED

The items to be searched consist of three electronic devices (collectively, the **TARGET DEVICES**) depicted below which were taken from PARK on April 17, 2025, and are currently in the possession of the FBI and located at 2100 Jamieson Avenue, Alexandria, VA 22314:

a. Apple iPhone 16 ProMax with no visible IMEI, in a blue case;

b. Samsung Galaxy, in a black Otterbox phone case, with IMEI 352512143400313; and

c. Samsung phone with IMEI 359186103322693, in a green Designskin phone case.

ATTACHMENT B

ITEMS TO BE SEIZED

All records and information, from October 1, 2018, through the present, that constitute evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. § 157 (Bankruptcy Fraud), 18 U.S.C. § 1343 (Wire Fraud), and 18 U.S.C. § 1956 (a)(1)(B)(i) (Concealment Money Laundering) (the "**SUBJECT OFFENSES**"), including:

1. all records containing information regarding bankruptcy fraud, wire fraud or money laundering;
2. information related to KOK Play and FileUp;
3. information related to communications with KOK Play, FileUp and all other cryptocurrency token investors, including complaints by investors or requests for the return of funds;
4. information related to the advertisement and promotion of KOK Play, FileUp and all other cryptocurrency tokens;
5. copies of bankruptcy documents and income tax returns filed with the Internal Revenue Service or Virginia Department of Revenue;
6. information related to financial transactions associated with Victim-1, Victim-2, Victim-3, S.J., and any other potential investors and/or co-conspirators, including all bank records, checks, credit card bills, account information, and other financial records, receipts for payment and disbursement of services;
7. any and all cryptocurrency, to include the following:
    a. any and all representations of cryptocurrency public keys or addresses, whether in electronic or physical format;

b. any and all representations of cryptocurrency private keys, whether in electronic or physical format; and

c. any and all representations of cryptocurrency wallets or their constitutive parts, whether in electronic or physical format, to include "recovery seeds" or "root keys" which may be used to regenerate a wallet.

Specifically, the United States is authorized to seize any and all cryptocurrency by transferring the full account balance in each wallet to a public cryptocurrency address controlled by the United States. The United States is further authorized to copy any wallet files and restore them onto computers controlled by the United States. By restoring the wallets on its own computers, the United States will continue to collect cryptocurrency transferred into the defendant's wallets as a result of transactions that were not yet completed at the time that the defendant's devices were seized.

8. all cryptocurrency records and account information, including information identifying addresses associated with investor and promoter virtual currency accounts and wallet addresses, stored on electronic and paper wallets or other means, cryptocurrency private keys and recovery seeds;

9. information related to receipt of investor money, including the amount, purpose of the investment, and plans for spending that money;

10. for any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

    a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited,

or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. evidence of the times the digital device or other electronic storage media was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

i. contextual information necessary to understand the evidence described in this attachment.

11. records and things evidencing the use of an Internet Protocol (IP) address to communicate with the internet, including:

a. routers, modems, and network equipment used to connect computers to the internet;

b. records of Internet Protocol addresses used;

c. records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

12. information identifying the identity of the person(s) who created or used the **TARGET DEVICES** including records that help reveal the whereabouts of such person(s);

13. evidence indicating the state of mind, e.g., intent, absence of mistake, or evidence indicating preparation or planning, as it relates to the criminal activity under investigation by individuals interacting with the **TARGET DEVICES**;

14. any communications with and/or relating to potential victims of the **SUBJECT OFFENSES**; and

15. any communications with and/or relating to co-conspirators of the **SUBJECT OFFENSES**.

As used above, the terms "records" and "information" include all of the forgoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of

information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

1. Surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
2. "Opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;
3. "Scanning" storage areas to discover and possible recover recently deleted files;
4. "Scanning" storage areas for deliberately hidden files; or
5. Performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.
6. If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take

appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

If the government identifies seized communications to or from an attorney, the investigative team will discontinue review until a filter team of government attorneys and agents is established. The filter team will have no previous or future involvement in the investigation of this matter. The filter team will review all seized communications and segregate communications to or from attorneys, which may or may not be subject to attorney-client privilege. At no time will the filter team advise the investigative team of the substance of any of the communications to or from attorneys. The filter team then will provide all communications that do not involve an attorney to the investigative team and the investigative team may resume its review. If the filter team decides that any of the communications to or from attorneys are not actually privileged (e.g., the communication includes a third party or the crime-fraud exception applies), the filter team

must obtain a court order before providing these attorney communications to the investigative team.